

REMARKS/ARGUMENTS

This case has been reviewed and analyzed in view of the Official Action dated 24 September 2004. Responsive to the rejections made by the Examiner in the outstanding Official Action, Claims 1-3 and 7 have now been amended and Claims 4-6 have been canceled from this case in order to more clearly clarify the inventive concept of the Applicant.

The Examiner has objected to Claim 4 under 37 C.F.R. § 1.75 as being a substantial duplicate of Claim 3. Claim 4 has now been canceled from this case.

The Examiner has further rejected Claims 1-2, 5-7 under 35 U.S.C. § 112, second paragraph, as being indefinite. Claims 1-3 and 7 have now been amended, following the Examiner's suggestions with regard to Claims 1 and 2, and further to correct grammatical, translational, and idiomatic errors. It is now believed that Claims 1-3 and 7 satisfy the requirements of 35 U.S.C. § 112, second paragraph.

The Examiner has additionally rejected Claims 1-4 and 7 under 35 U.S.C. § 102(e) as being anticipated by the Puhl Patent #6,223,291. It is the Examiner's contention that all elements of Claims 1-4 and 7, as originally filed, are taught by the Puhl reference.

The Puhl reference is directed to a secure wireless electronic-commerce system with digital product certificates and digital license certificates. The Puhl reference teaches an end-to-end real-time encoding module for WAP data transmission wherein the encryption code security system of the Puhl reference includes a public key infrastructure

installed in a WML server end of a mobile server of a wireless service provider and, further, where the WML server is the WAP proxy server which serves as a WML server translating HTML to WML.

The Puhl reference, however, does not teach or even suggest the use of a randomly generated key. A randomizing key generating process provides for optimal security in that there is no algorithm which may be illicitly utilized for guessing or generating keys which should remain secure. Further, the Puhl reference does not teach or suggest the use of a pre-compressor for compression of transmission data, which allows the general processing system to be alleviated from both excessive computational time and resources.

The system of the subject Patent Application, however, includes a key management system for randomly generating an ideal key. The key management system uses a randomizing process in order to provide an optimally secure key for encryption. Further, the key management system performs a secret sharing process wherein the original key is divided into a plurality of “key shadows”, with the original key being restored only when a selected number of key shadows are combined, thus providing extra security for the key generation and utilization system.

The system of the subject Patent Application further includes a pre-compressor for dividing original data into a plurality of unit character strings, converting the data through a variety of decimal-to-hexadecimal processes and, eventually, converting each character code into a respective ANSI character set. This saves computational time and energy

from the main processing system in that these processes are carried out by the pre-compressor for the compression of the transmission data.

Thus, the Puhl reference does not include: "...said key management randomly generating an ideal key, said ideal key being stored and held secretly, said key management further generating a second set of keys which are in high demand and are frequently updated by a pseudo-random process, said key management further performing a secret sharing process wherein an original key is divided into a plurality of key shadows...a pre-compressor for compression of transmission data...", as is clearly provided by newly-amended Independent Claim 1.

Thus, it is not believed that the subject Application is anticipated by, or made obvious by, the Puhl reference when Independent Claim 1 is carefully reviewed.

The Examiner has additionally rejected Claim 5 under 35 U.S.C. § 103(a) as being unpatentable over the Puhl reference and the Schneier "Applied Cryptography" reference. It is the Examiner's contention that it would have been obvious to one of ordinary skill in the art to use the key generation and backup techniques of Schneier in order to generate keys that are difficult to guess and prevent the loss of encrypted data if the key is accidentally lost.

The Schneier reference is directed to the generation of public keys from private keys and the related encryption. Though the Schneier reference does suggest the use of

random-bit strings generated “by some automatic process”, it does not teach or suggest the use of a pseudo-random process.

The system of the subject Patent Application, in contradistinction, includes a key management which generates a second set of keys which are in high demand and are frequently updated, with the generation of the second set of keys being performed by a pseudo-random process. The pseudo-random process follows a significantly different algorithm than a randomizer and, in general, pseudo-random processes do not require as much processing energy or time as a true randomizer. The second set of keys, which is not taught or suggested by the Schneier reference, is for a set of keys which are in high demand by the system and require frequent updating. The Schneier reference does not teach or suggest the separation of keys based upon their demand or the rate of updating required.

Thus, neither the Schneier reference nor the Puhl reference, when taken alone or in combination, include: “...said key management further generating a second set of keys which are in high demand and are frequently updated by a pseudo-random process...”, as is clearly provided by newly-amended Independent Claim 1.

Thus, based upon newly-amended Independent Claim 1, it is not believed that the subject Patent Application is made obvious by either the Puhl reference or the Schneier reference, when taken alone or in combination.

The Examiner has further rejected Claim 6 under 35 U.S.C. § 103(a) as being unpatentable over Puhl. It is the Examiner's contention that the pre-compressor process was well-known in the art at the time of the invention.

The Puhl reference, however, as noted above with regard to the rejection under 35 U.S.C. § 102, does not teach or suggest the use of a key management system or the random generation of an ideal key. Further, the Puhl reference does not teach or suggest a key management system which generates a second set of keys being in high demand and frequently updated, with the second set of keys being generated by a pseudo-random process, as discussed above with regard to the rejection under the Schneier reference in combination with the Puhl reference.

Further, though the compression transmission data is well-known in the art, the Puhl reference does not teach or suggest the use of a separate pre-compressor for the compression of transmission data, allowing for relief of computational time and energy from the main processing system.

The system of the subject Patent Application includes a pre-compressor for the compression of transmission data, allowing for relief of computational time and energy from the main processing system, which increases the efficiency of the generation of the keys.

Thus, the Puhl reference does not include: "...said key management randomly generating an ideal key, said ideal key being stored and held secretly, said key

MR2349-600

Application Serial No. 09/804,258

Responsive to Office Action dated 24 September 2004

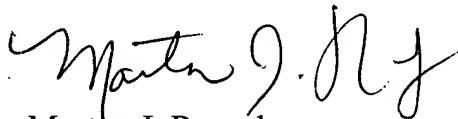
management further generating a second set of keys which are in high demand and are frequently updated by a pseudo-random process...a pre-compressor for compression of transmission data...”, as is clearly provided by newly-amended Independent Claim 1.

Thus, based upon newly-amended Independent Claim 1, it is not believed that the subject Patent Application is made obvious by the Puhl reference when Independent Claim 1 is carefully reviewed.

It is now believed that the remaining Claims 2, 3, and 7 show patentable distinction over the prior art cited by the Examiner for at least the same reasons as those previously discussed for Independent Claim 1.

It is now believed that the subject Patent Application has been placed in condition for allowance, and such action is respectfully requested.

Respectfully submitted,



Morton J. Rosenberg
Registration #26,049

Dated: 1/19/05

Rosenberg, Klein & Lee
3458 Ellicott Center Drive
Suite 101
Ellicott City, MD 21043
410-465-6678